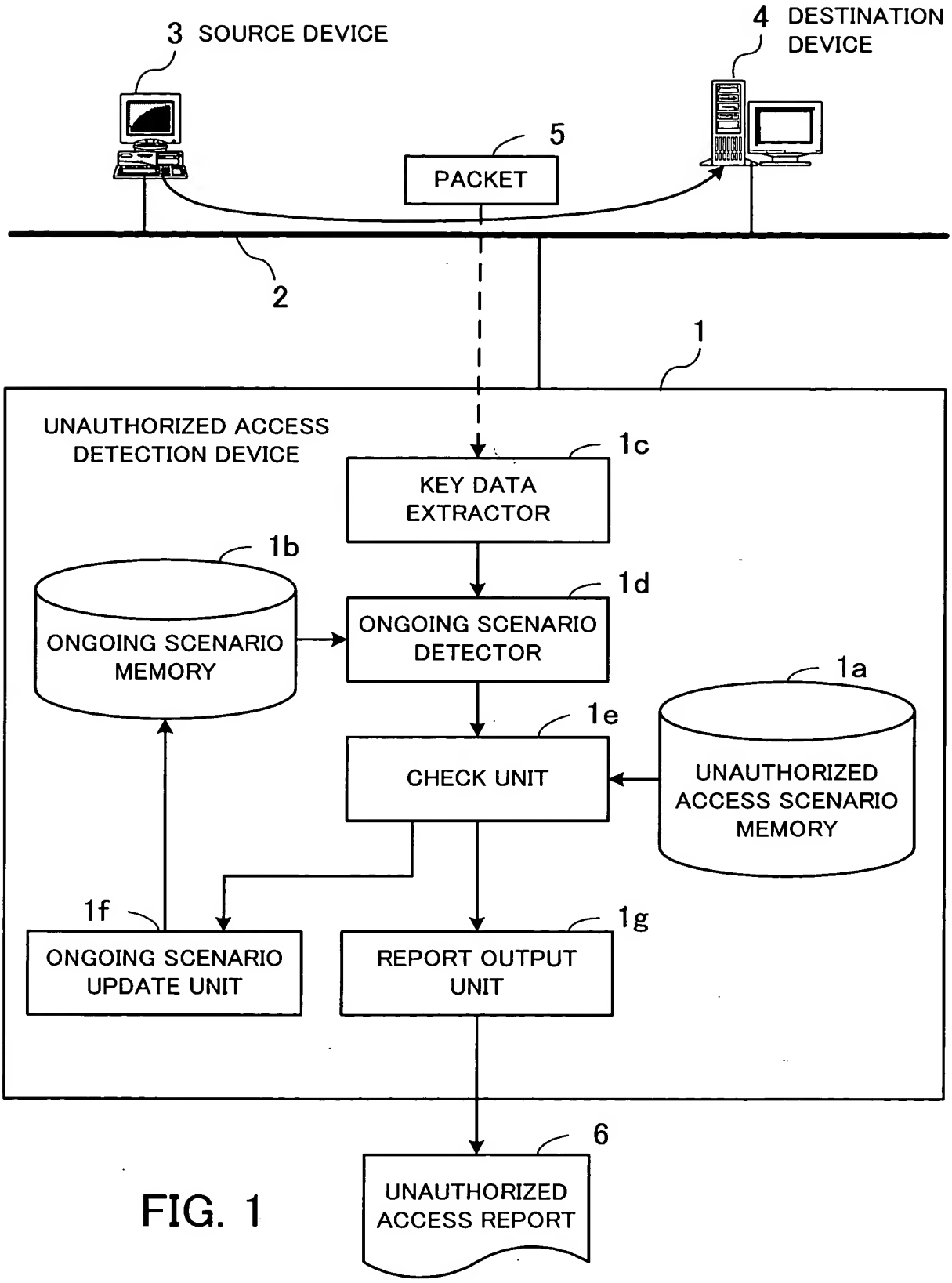

3 SOURCE DEVICE
4 DESTINATION DEVICE
5
PACKET
2
1
UNAUTHORIZED ACCESS DETECTION DEVICE
1c
KEY DATA EXTRACTOR
1b
ONGOING SCENARIO MEMORY
1d
ONGOING SCENARIO DETECTOR
1a
1e
CHECK UNIT
UNAUTHORIZED ACCESS SCENARIO MEMORY
1f
ONGOING SCENARIO UPDATE UNIT
1g
REPORT OUTPUT UNIT
6
UNAUTHORIZED ACCESS REPORT

FIG. 1

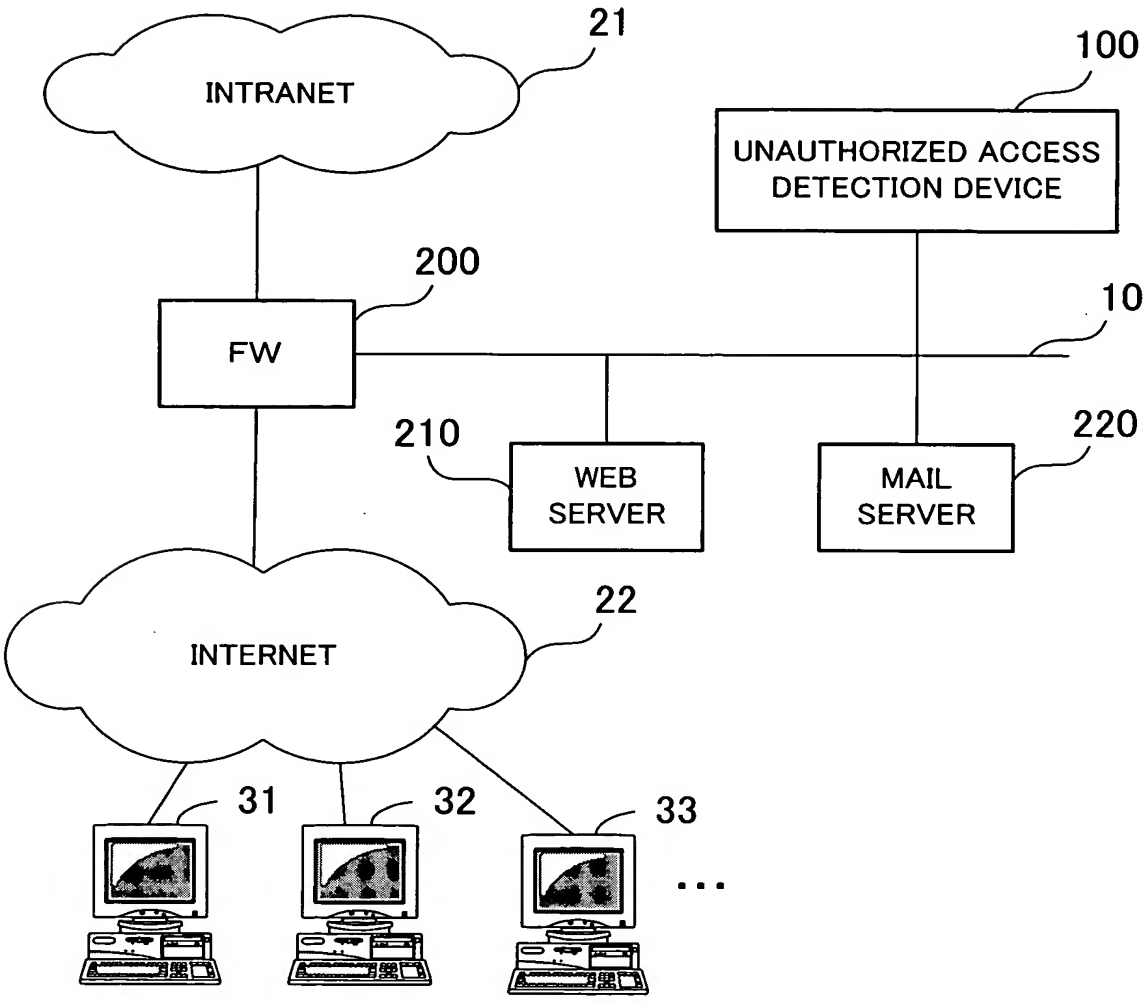

21
INTRANET
100
UNAUTHORIZED ACCESS DETECTION DEVICE
200
FW
10
210
WEB SERVER
220
MAIL SERVER
22
INTERNET
31
32
33
...

FIG. 2

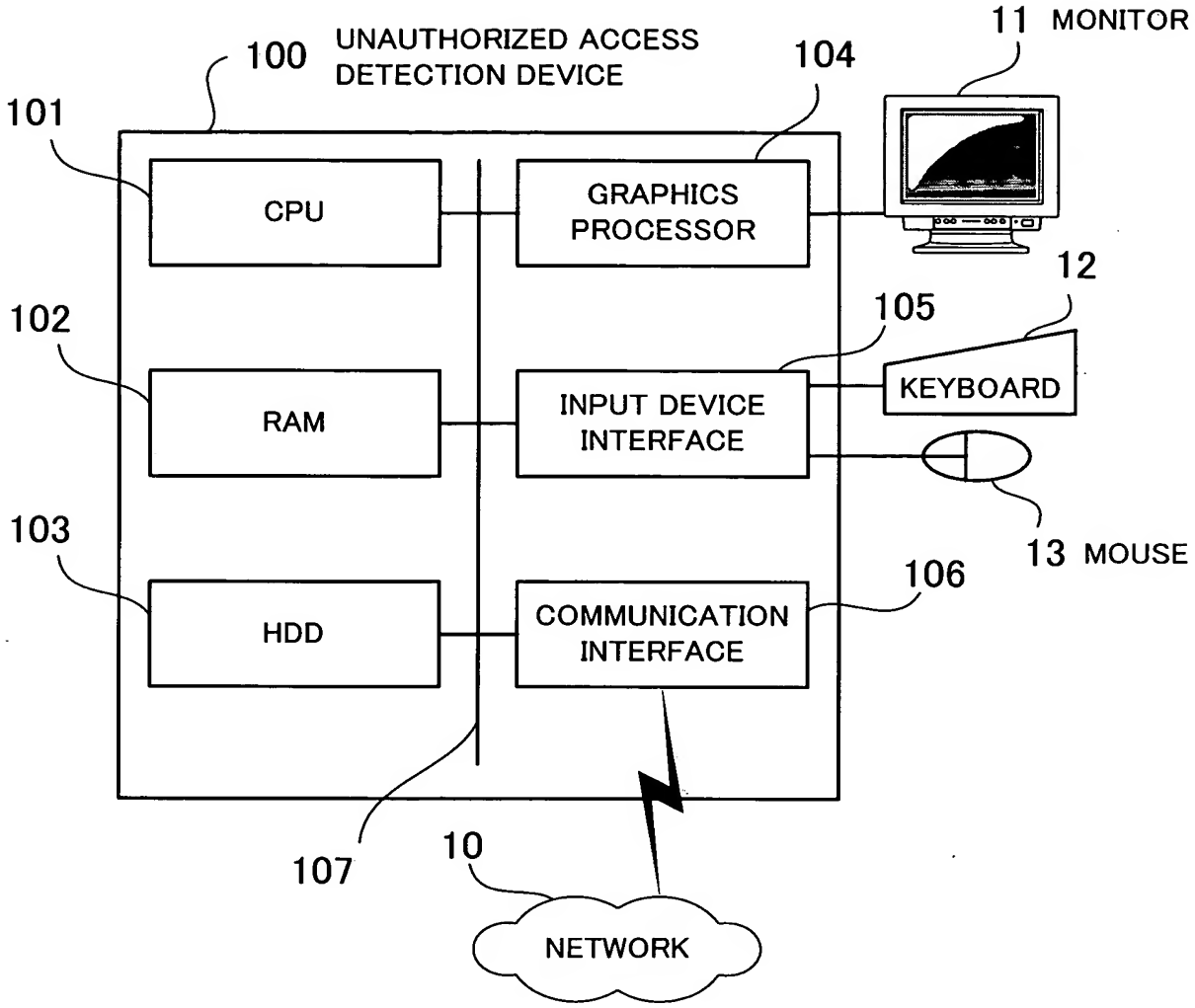

11 MONITOR
100 UNAUTHORIZED ACCESS DETECTION DEVICE
104
101
CPU
GRAPHICS PROCESSOR
12
105
102
RAM
INPUT DEVICE INTERFACE
KEYBOARD
13 MOUSE
103
106
HDD
COMMUNICATION INTERFACE
107
10
NETWORK

FIG. 3

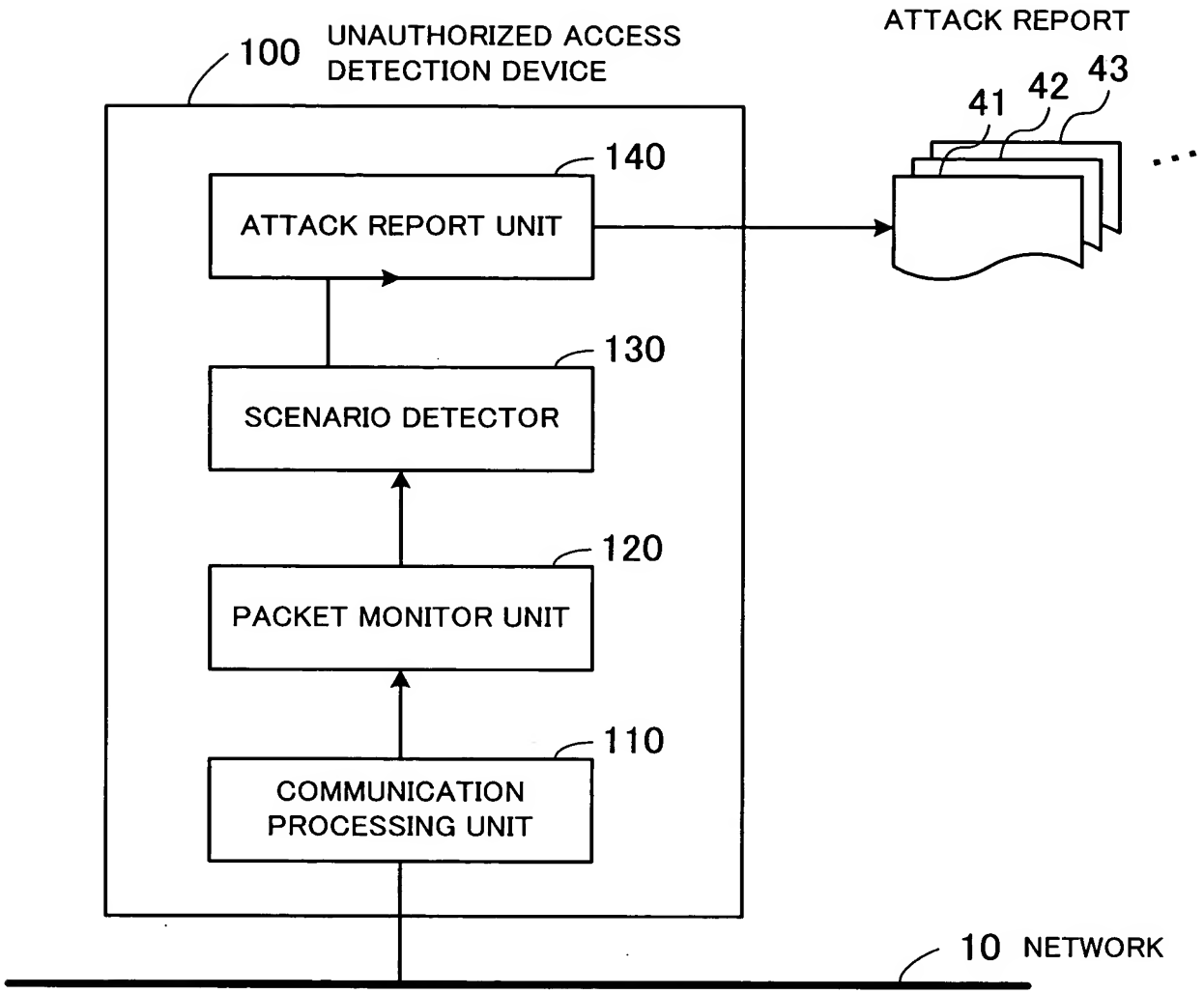

100
UNAUTHORIZED ACCESS DETECTION DEVICE
ATTACK REPORT
41
42
43
140
ATTACK REPORT UNIT
130
SCENARIO DETECTOR
120
PACKET MONITOR UNIT
110
COMMUNICATION PROCESSING UNIT
10
NETWORK

FIG. 4

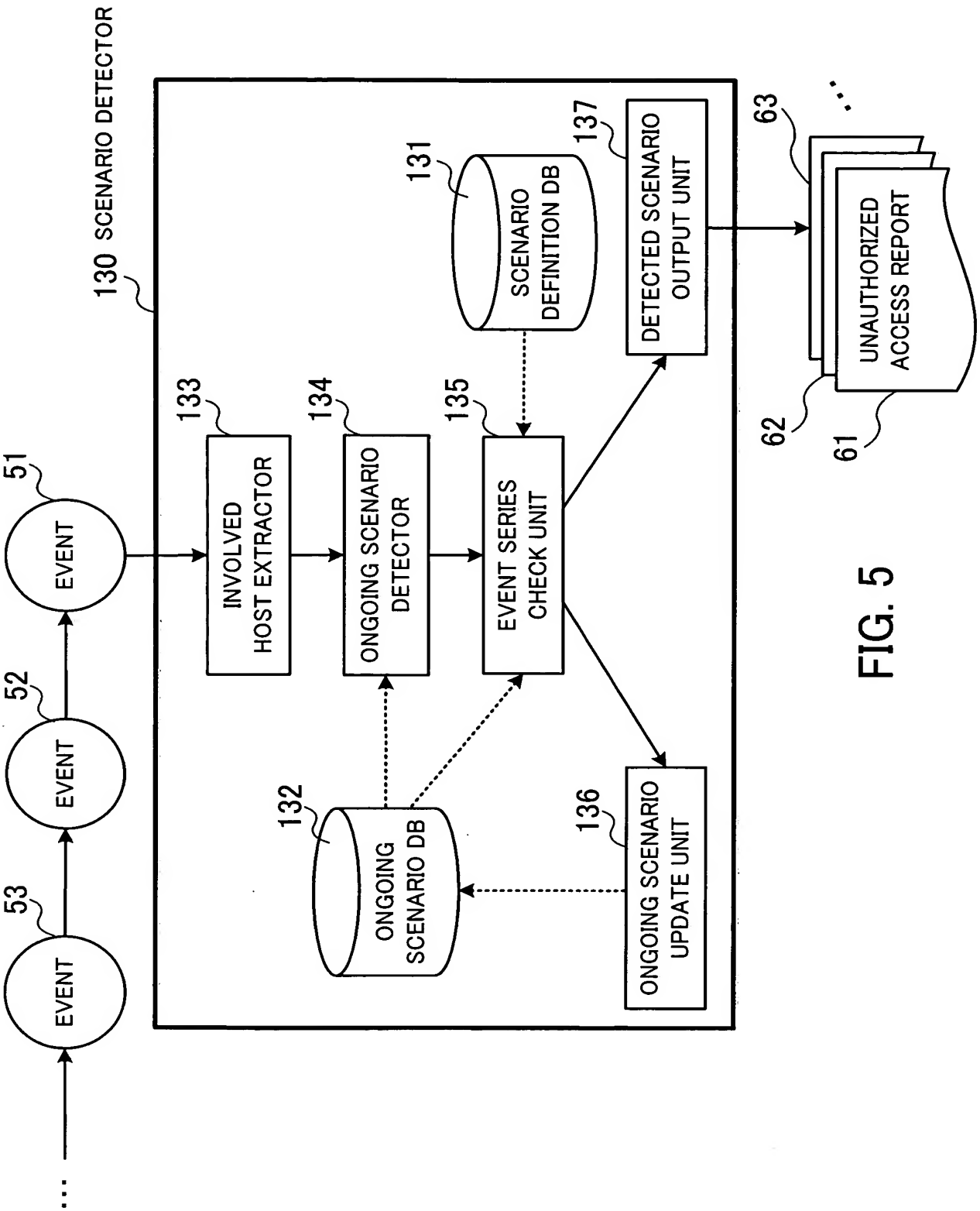

130 SCENARIO DETECTOR
51
EVENT
52
EVENT
53
EVENT
...
133
INVOLVED HOST EXTRACTOR
134
ONGOING SCENARIO DETECTOR
135
EVENT SERIES CHECK UNIT
131
SCENARIO DEFINITION DB
137
DETECTED SCENARIO OUTPUT UNIT
132
ONGOING SCENARIO DB
136
ONGOING SCENARIO UPDATE UNIT
63
62
61
UNAUTHORIZED ACCESS REPORT
...

FIG. 5

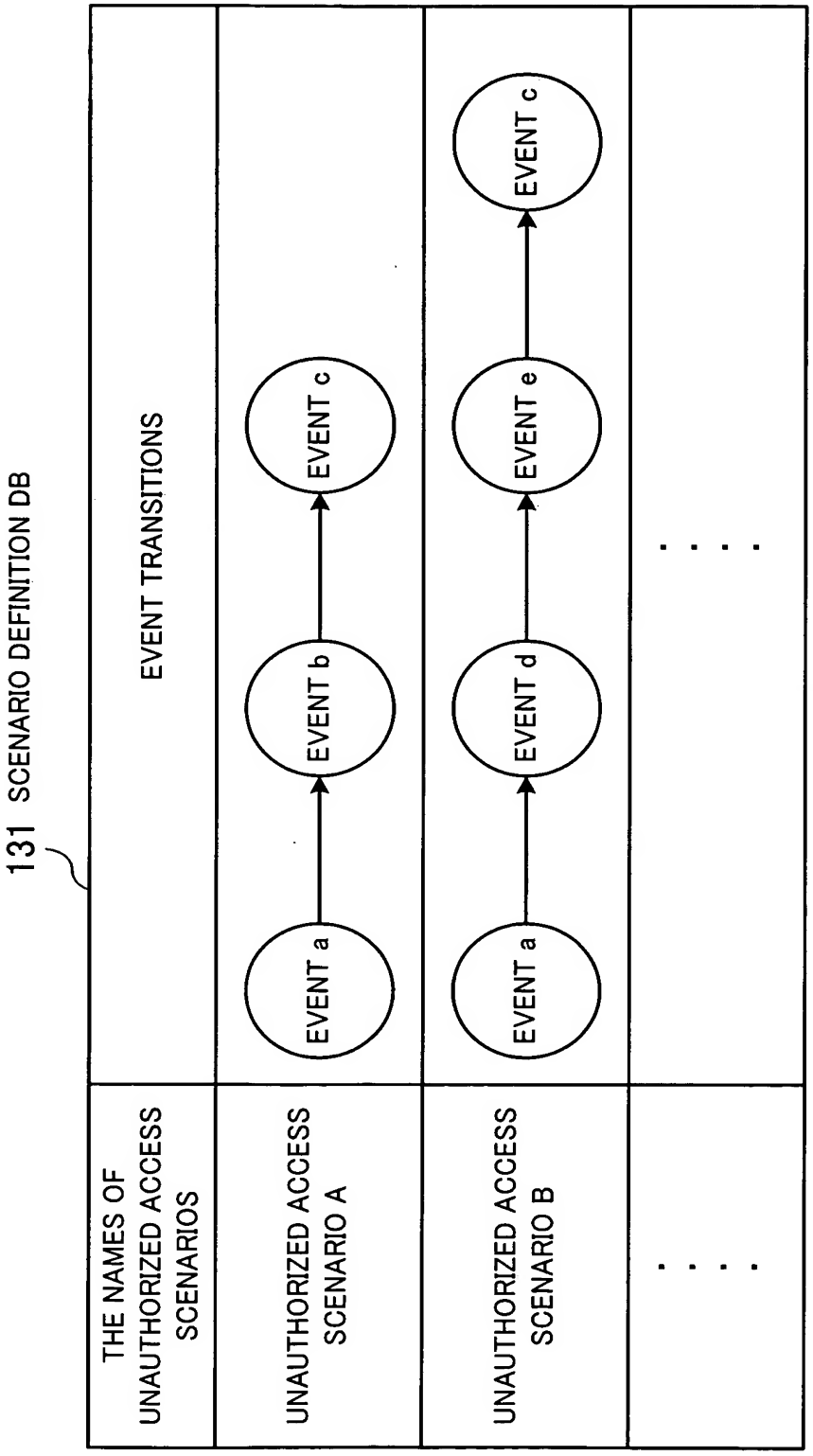

131 SCENARIO DEFINITION DB
THE NAMES OF UNAUTHORIZED ACCESS SCENARIOS
EVENT TRANSITIONS
UNAUTHORIZED ACCESS SCENARIO A
EVENT a
EVENT b
EVENT c
UNAUTHORIZED ACCESS SCENARIO B
EVENT a
EVENT d
EVENT e
EVENT c

FIG. 6

132 ONGOING SCENARIO DB

PAIRS OF SOURCE IP ADDRESS AND DESTINATION IP ADDRESS	NAME OF UNAUTHORIZED ACCESS SCENARIO	DEGREE OF PROGRESS
192.168.1.5→10.10.100.100	UNAUTHORIZED ACCESS SCENARIO B	SECOND STAGE
10.1.1.123→192.168.30.30	UNAUTHORIZED ACCESS SCENARIO D	THIRD STAGE
. . .	. . .	. . .

FIG. 7

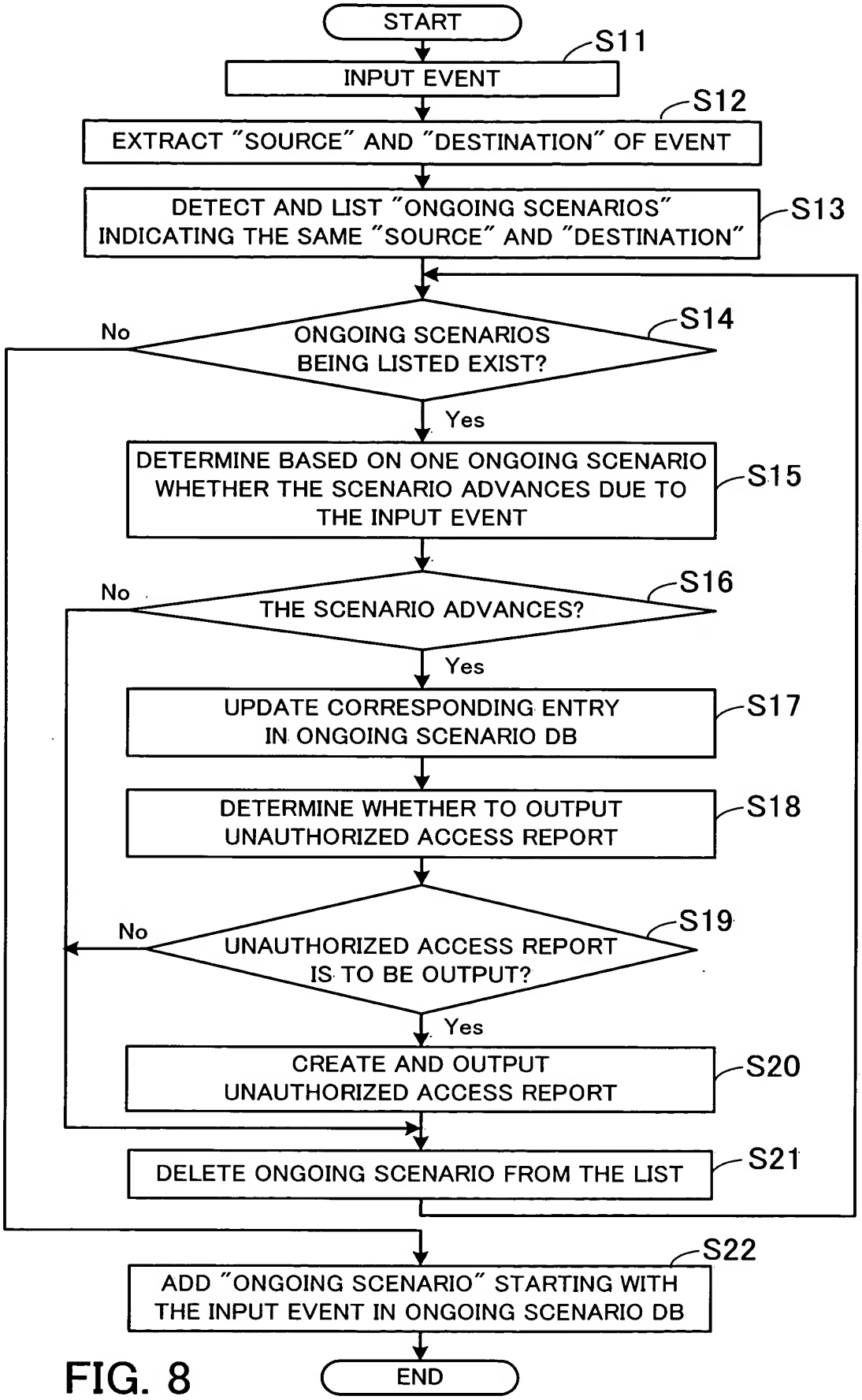

START
S11
INPUT EVENT
S12
EXTRACT "SOURCE" AND "DESTINATION" OF EVENT
DETECT AND LIST "ONGOING SCENARIOS" INDICATING THE SAME "SOURCE" AND "DESTINATION"
S13
S14
No
ONGOING SCENARIOS BEING LISTED EXIST?
Yes
DETERMINE BASED ON ONE ONGOING SCENARIO WHETHER THE SCENARIO ADVANCES DUE TO THE INPUT EVENT
S15
S16
No
THE SCENARIO ADVANCES?
Yes
UPDATE CORRESPONDING ENTRY IN ONGOING SCENARIO DB
S17
DETERMINE WHETHER TO OUTPUT UNAUTHORIZED ACCESS REPORT
S18
S19
No
UNAUTHORIZED ACCESS REPORT IS TO BE OUTPUT?
Yes
CREATE AND OUTPUT UNAUTHORIZED ACCESS REPORT
S20
DELETE ONGOING SCENARIO FROM THE LIST
S21
S22
ADD "ONGOING SCENARIO" STARTING WITH THE INPUT EVENT IN ONGOING SCENARIO DB
END

FIG. 8

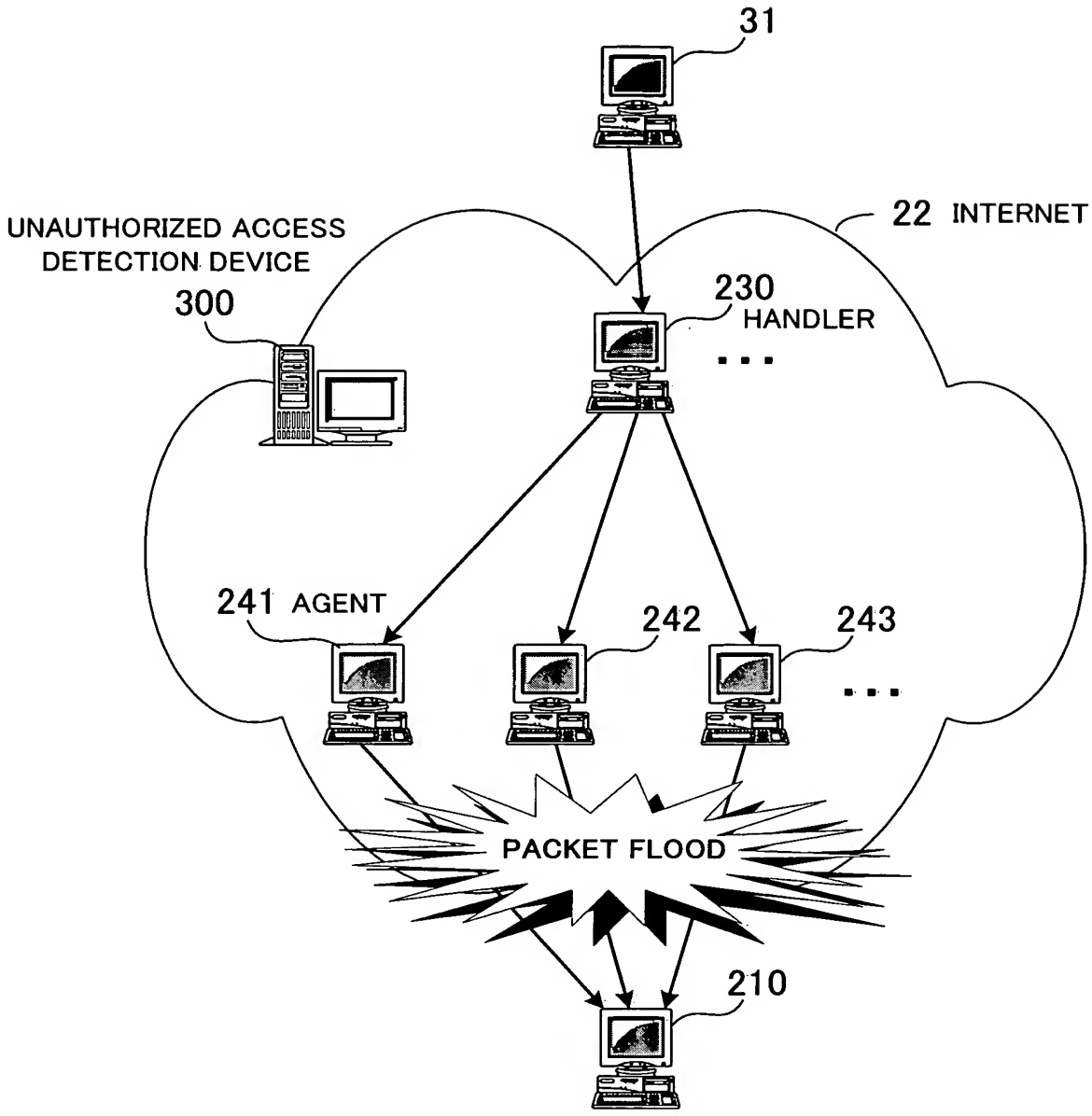

31
22 INTERNET
UNAUTHORIZED ACCESS
DETECTION DEVICE
300
230
HANDLER
241 AGENT
242
243
PACKET FLOOD
210

FIG. 9

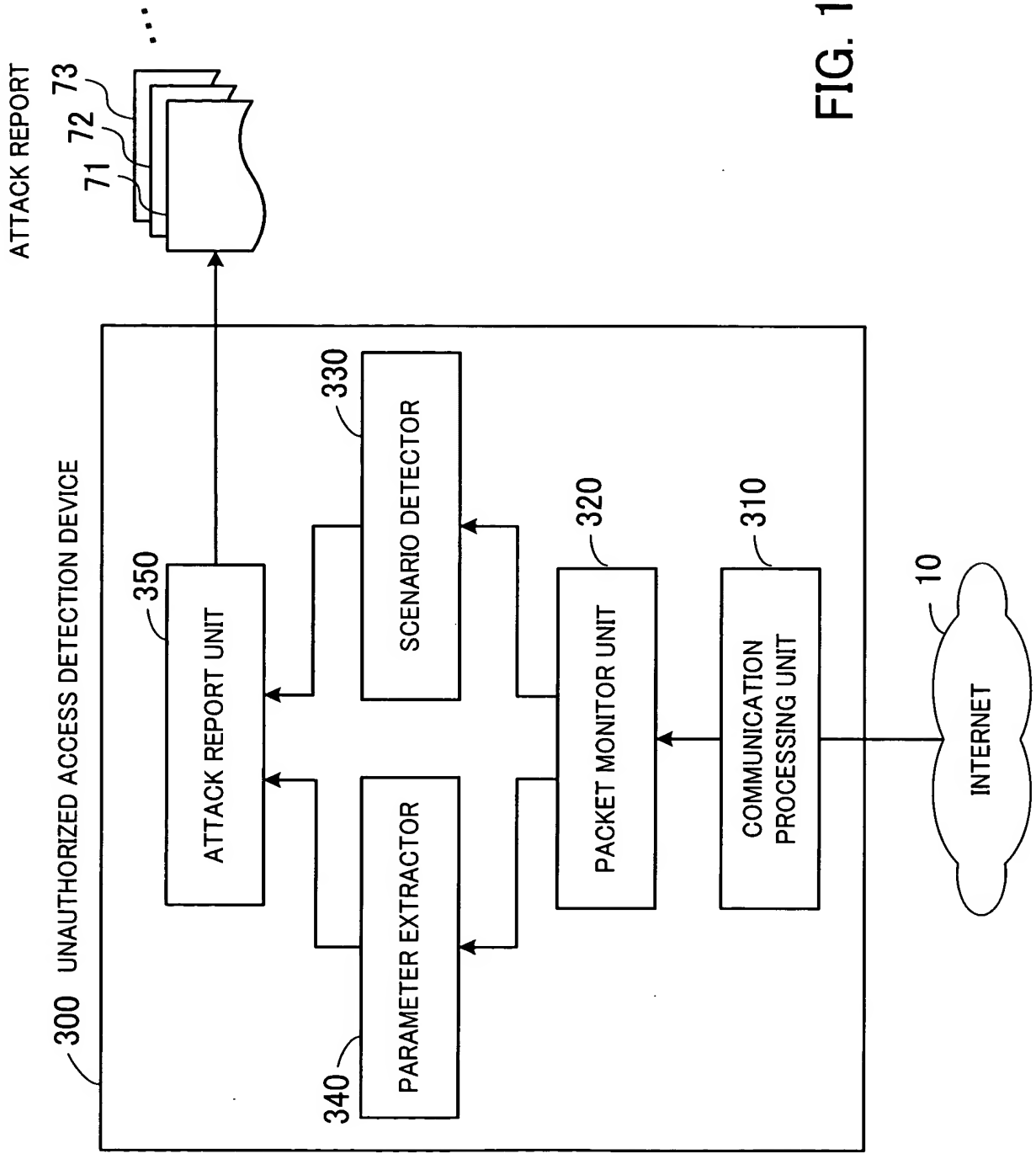

ATTACK REPORT
71
72
73
300 UNAUTHORIZED ACCESS DETECTION DEVICE
350
ATTACK REPORT UNIT
330
SCENARIO DETECTOR
340
PARAMETER EXTRACTOR
320
PACKET MONITOR UNIT
310
COMMUNICATION PROCESSING UNIT
10
INTERNET

FIG. 10

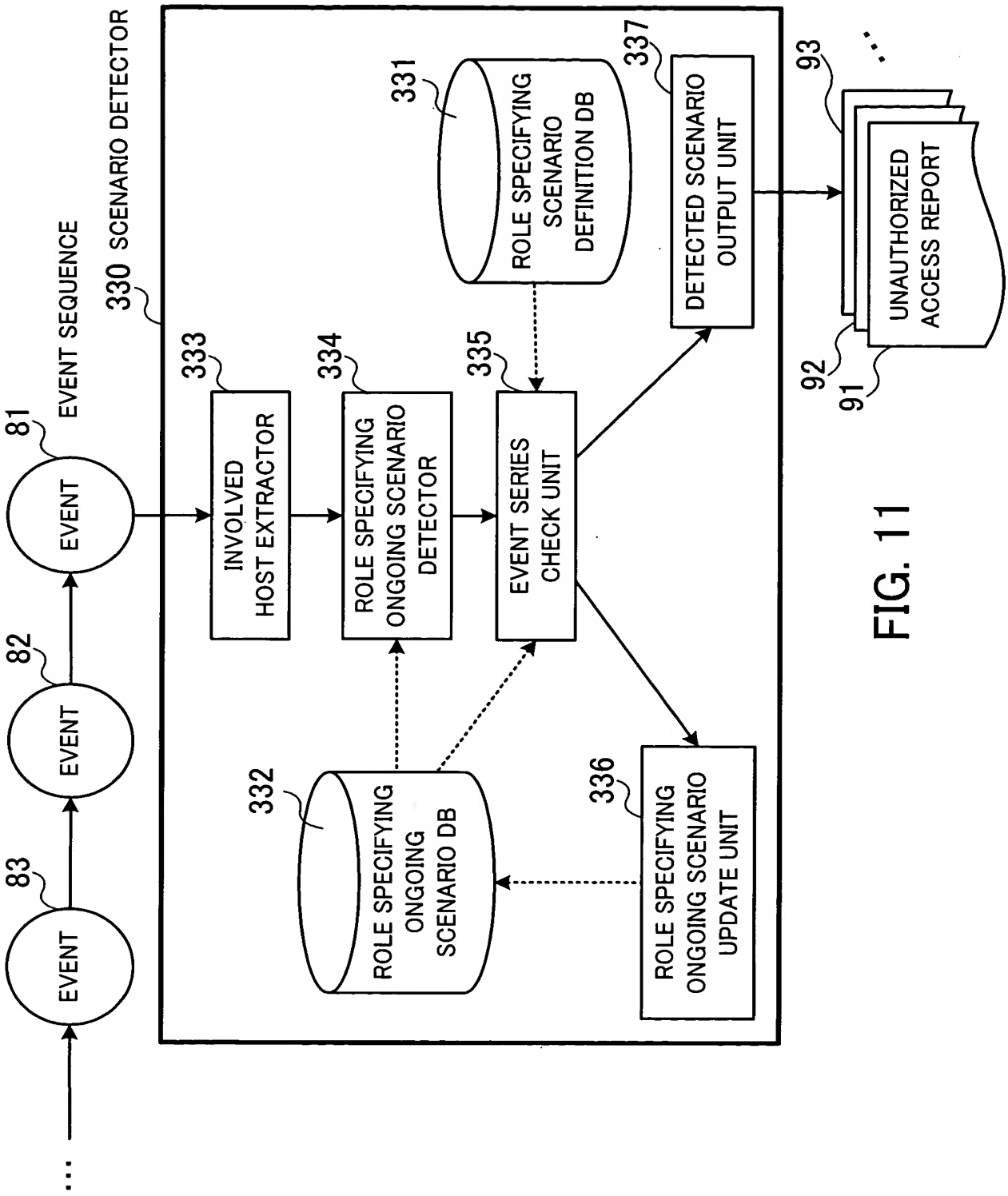

EVENT SEQUENCE
330 SCENARIO DETECTOR
81
82
83
EVENT
EVENT
EVENT
...
333
INVOLVED HOST EXTRACTOR
334
ROLE SPECIFYING ONGOING SCENARIO DETECTOR
335
EVENT SERIES CHECK UNIT
331
ROLE SPECIFYING SCENARIO DEFINITION DB
337
DETECTED SCENARIO OUTPUT UNIT
332
ROLE SPECIFYING ONGOING SCENARIO DB
336
ROLE SPECIFYING ONGOING SCENARIO UPDATE UNIT
92
91
93
UNAUTHORIZED ACCESS REPORT

FIG. 11

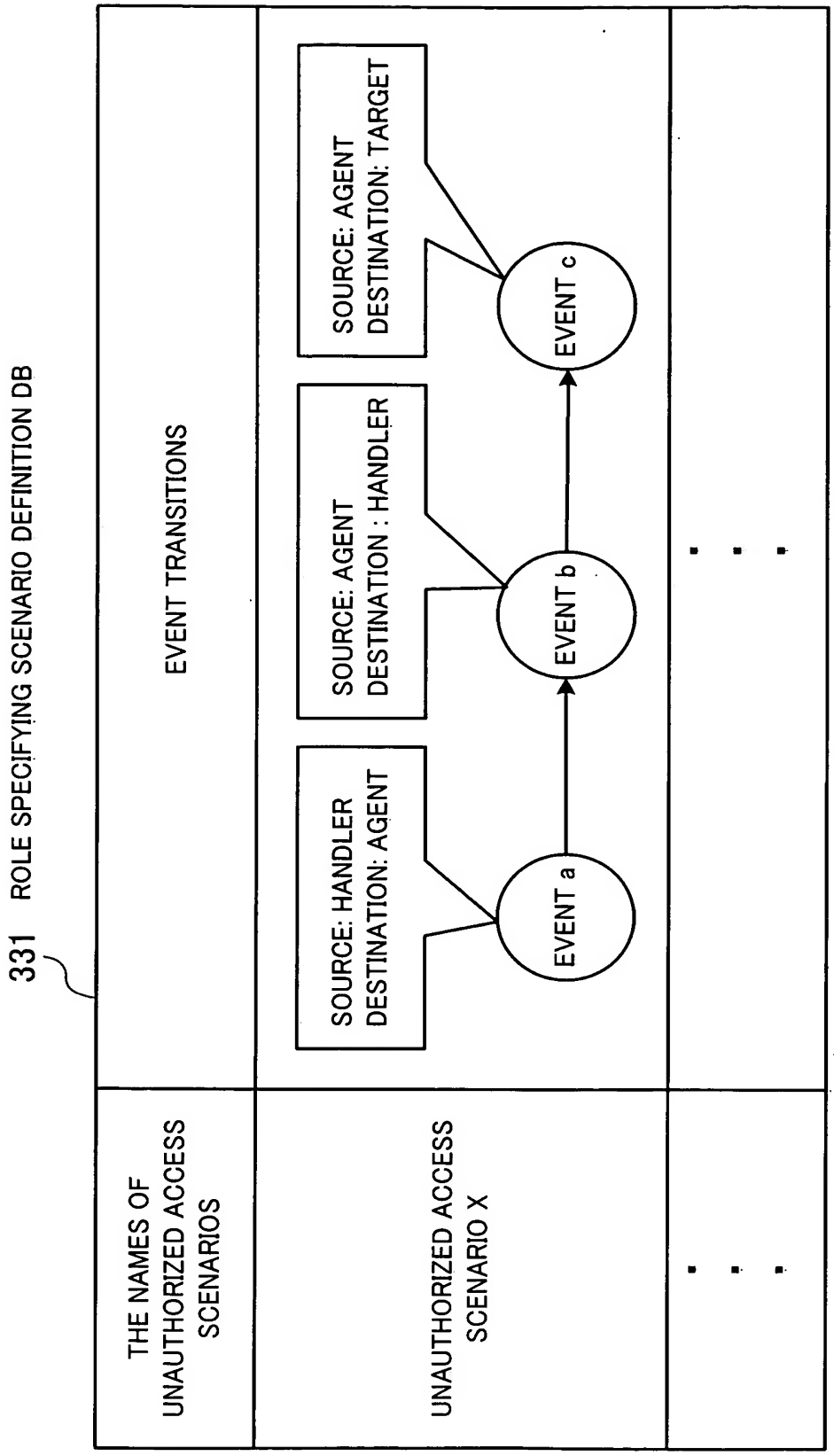

331 ROLE SPECIFYING SCENARIO DEFINITION DB
THE NAMES OF UNAUTHORIZED ACCESS SCENARIOS
EVENT TRANSITIONS
UNAUTHORIZED ACCESS SCENARIO X
SOURCE: HANDLER DESTINATION: AGENT
SOURCE: AGENT DESTINATION : HANDLER
SOURCE: AGENT DESTINATION: TARGET
EVENT a
EVENT b
EVENT c

FIG. 12

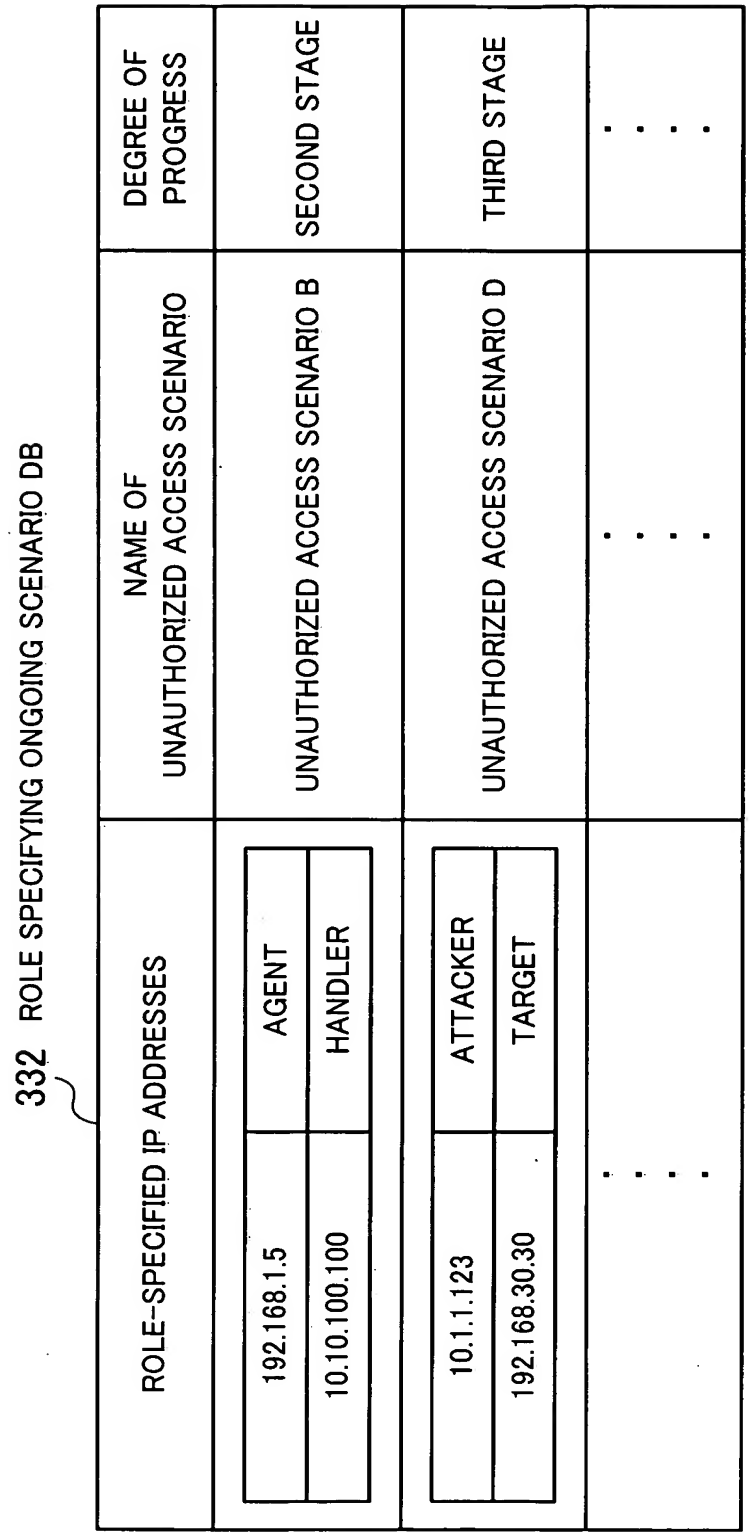

332 ROLE SPECIFYING ONGOING SCENARIO DB
ROLE-SPECIFIED IP ADDRESSES
NAME OF UNAUTHORIZED ACCESS SCENARIO
DEGREE OF PROGRESS
192.168.1.5
AGENT
10.10.100.100
HANDLER
UNAUTHORIZED ACCESS SCENARIO B
SECOND STAGE
10.1.1.123
ATTACKER
192.168.30.30
TARGET
UNAUTHORIZED ACCESS SCENARIO D
THIRD STAGE

FIG. 13

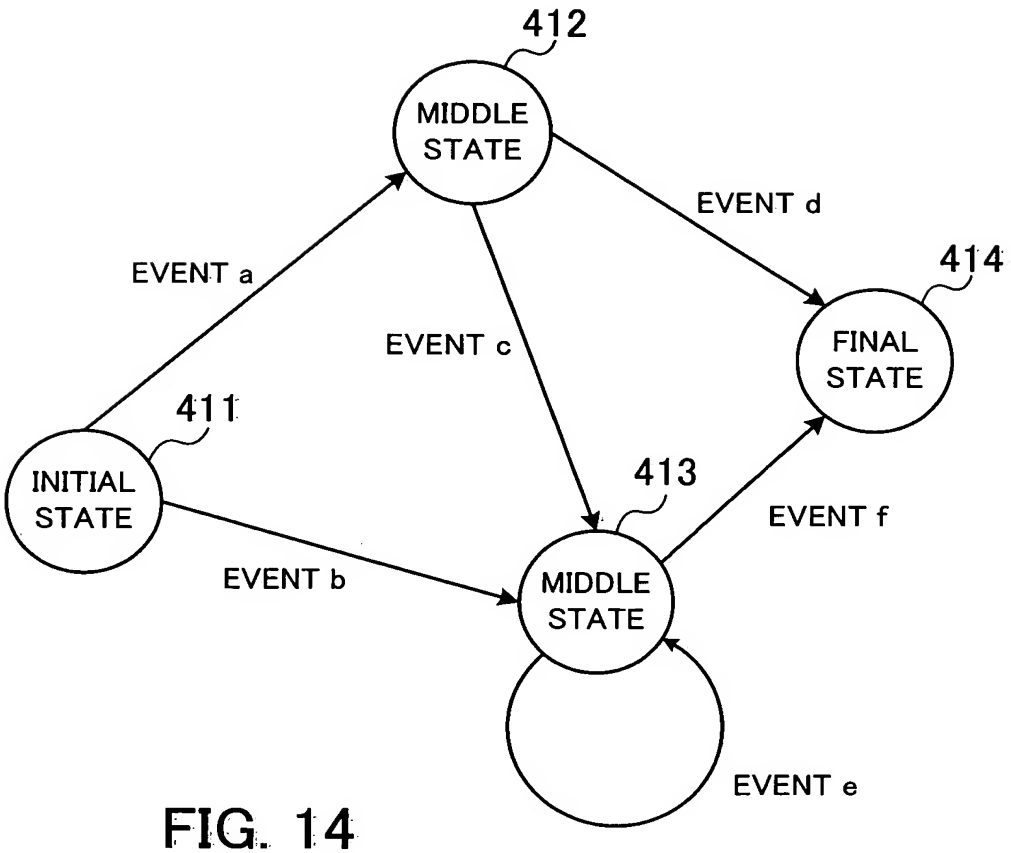

412
MIDDLE STATE
EVENT d
414
EVENT a
EVENT c
FINAL STATE
411
INITIAL STATE
413
EVENT f
EVENT b
MIDDLE STATE
EVENT e

FIG. 14

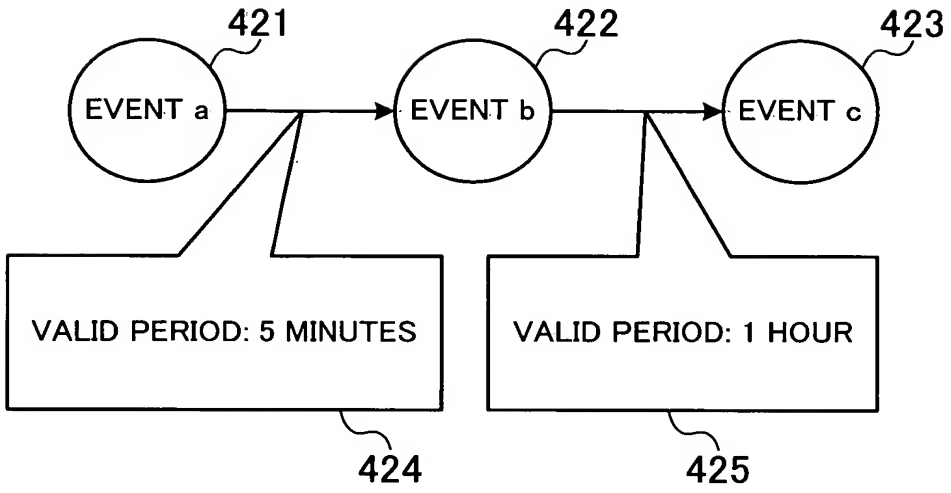
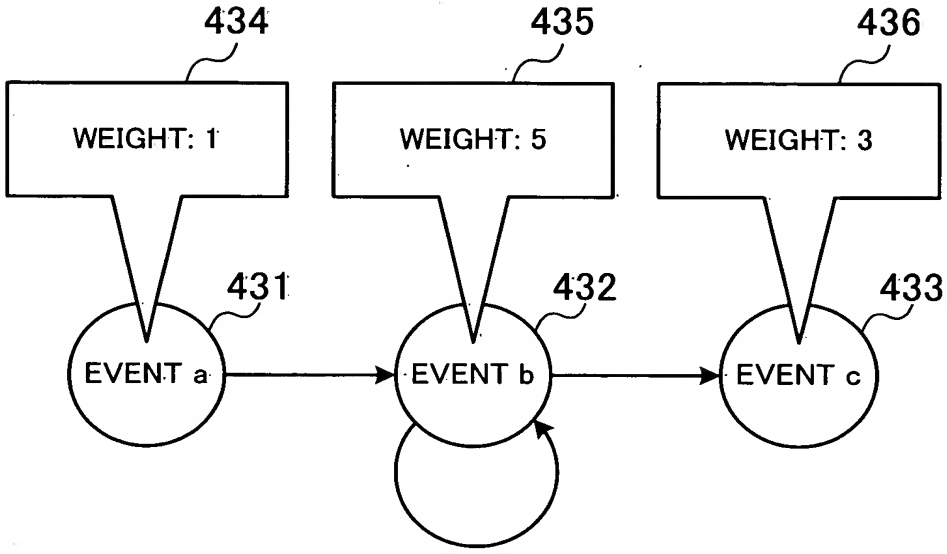

421
422
423
EVENT a
EVENT b
EVENT c
VALID PERIOD: 5 MINUTES
VALID PERIOD: 1 HOUR
424
425

FIG. 15



REPORT OUTPUT THRESHOLD VALUE: 8

FIG. 16

132a ONGOING SCENARIO DB

PAIRS OF SOURCE IP ADDRESS AND DESTINATION IP ADDRESS	NAME OF UNAUTHORIZED ACCESS SCENARIO	TOTAL WEIGHT
192.168.1.5→10.10.100.100	UNAUTHORIZED ACCESS SCENARIO B	6
10.1.1.123→192.168.30.30	UNAUTHORIZED ACCESS SCENARIO D	1
. . .	. . .	. . .

FIG. 17

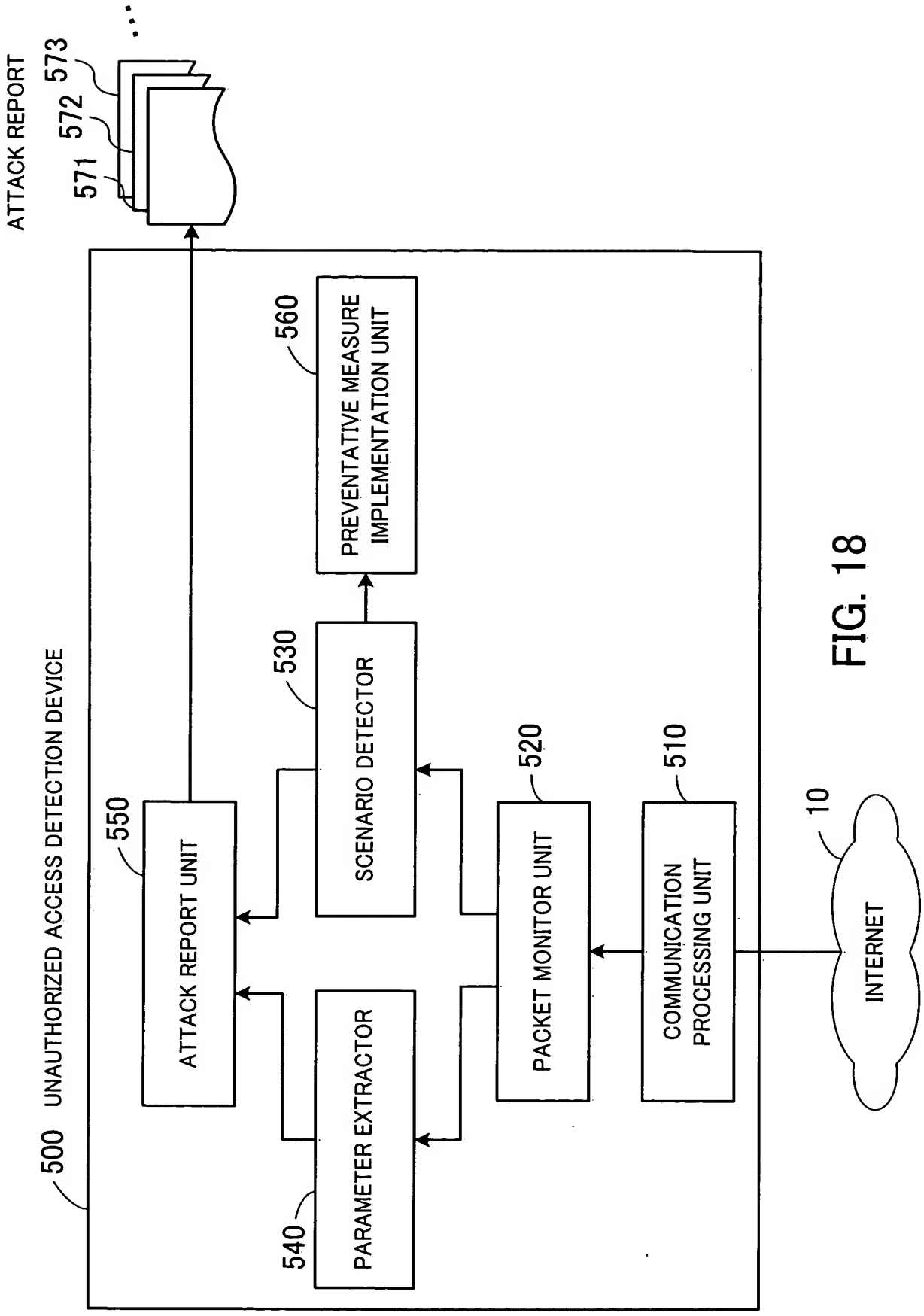

ATTACK REPORT
571
572
573
500
UNAUTHORIZED ACCESS DETECTION DEVICE
550
ATTACK REPORT UNIT
530
SCENARIO DETECTOR
560
PREVENTATIVE MEASURE IMPLEMENTATION UNIT
540
PARAMETER EXTRACTOR
520
PACKET MONITOR UNIT
510
COMMUNICATION PROCESSING UNIT
10
INTERNET

FIG. 18

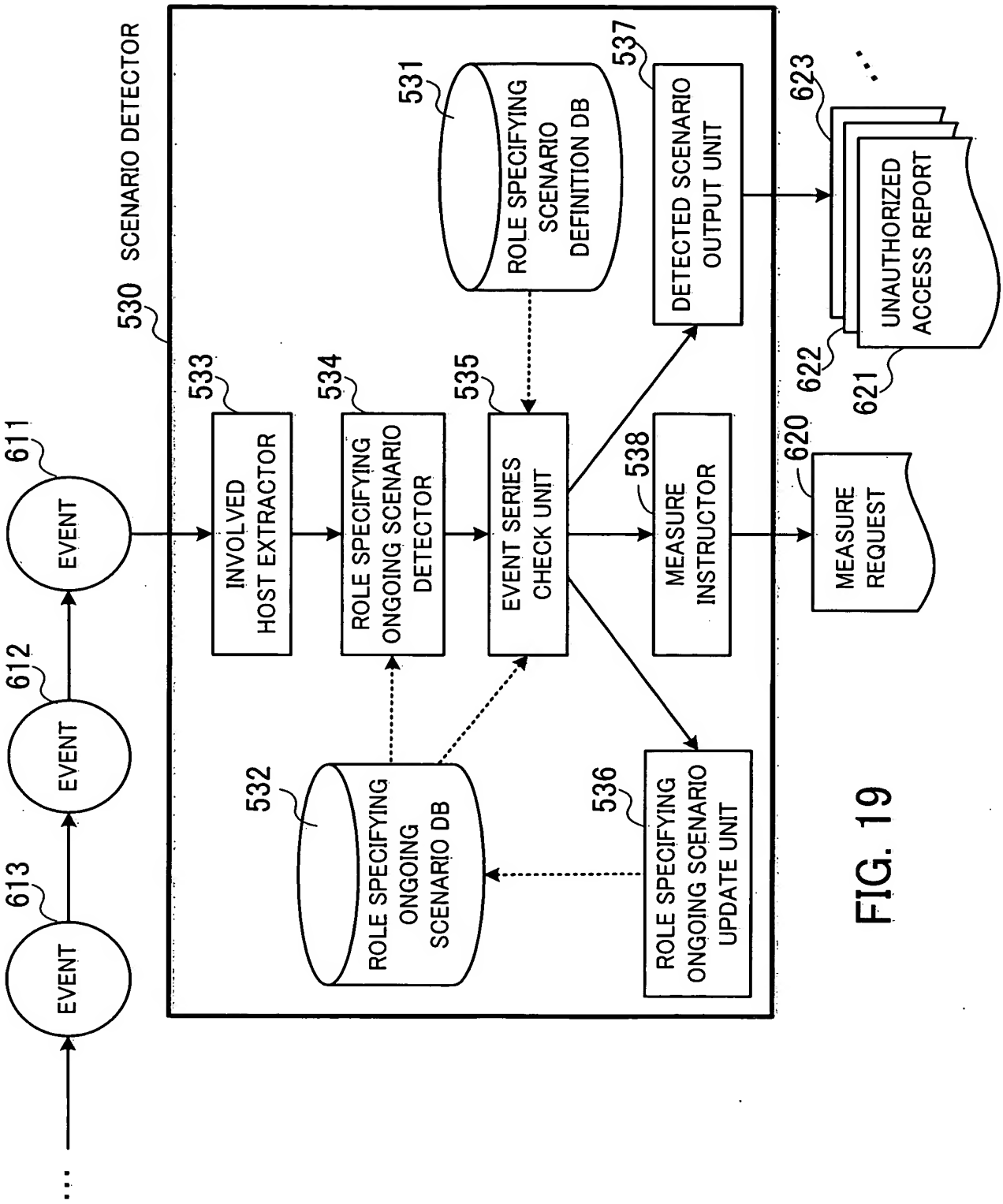

SCENARIO DETECTOR
530
EVENT
611
EVENT
612
EVENT
613
INVOLVED HOST EXTRACTOR
533
ROLE SPECIFYING ONGOING SCENARIO DETECTOR
534
EVENT SERIES CHECK UNIT
535
ROLE SPECIFYING SCENARIO DEFINITION DB
531
ROLE SPECIFYING ONGOING SCENARIO DB
532
ROLE SPECIFYING ONGOING SCENARIO UPDATE UNIT
536
DETECTED SCENARIO OUTPUT UNIT
537
MEASURE INSTRUCTOR
538
MEASURE REQUEST
620
UNAUTHORIZED ACCESS REPORT
621
622
623

FIG. 19

COMMANDS TO HANDLER	COMMANDS TO AGENT	DESCRIPTION
msize	rsz	SET THE SIZE (BYTE) OF A UDP PACKET TO BE USED FOR FUTURE FLOOD WITH A PARAMETER
mtimer	bbb	SET THE LENGTH (SECONDS) OF FUTURE FLOOD WITH A PARAMETER
mping	png	CONFIRM WHETHER EACH AGENT IS ALIVE OR NOT
die	d1e	STOP ALL AGENTS
dos	aaa	SEND UDP FLOOD TO IP ADDRESS SPECIFIED BY PARAMETER
mdos	xyz	SEND UDP FLOOD TO IP ADDRESS SPECIFIED BY PARAMETER. A PLURALITY OF IP ADDRESS CAN BE SPECIFIED

FIG. 20

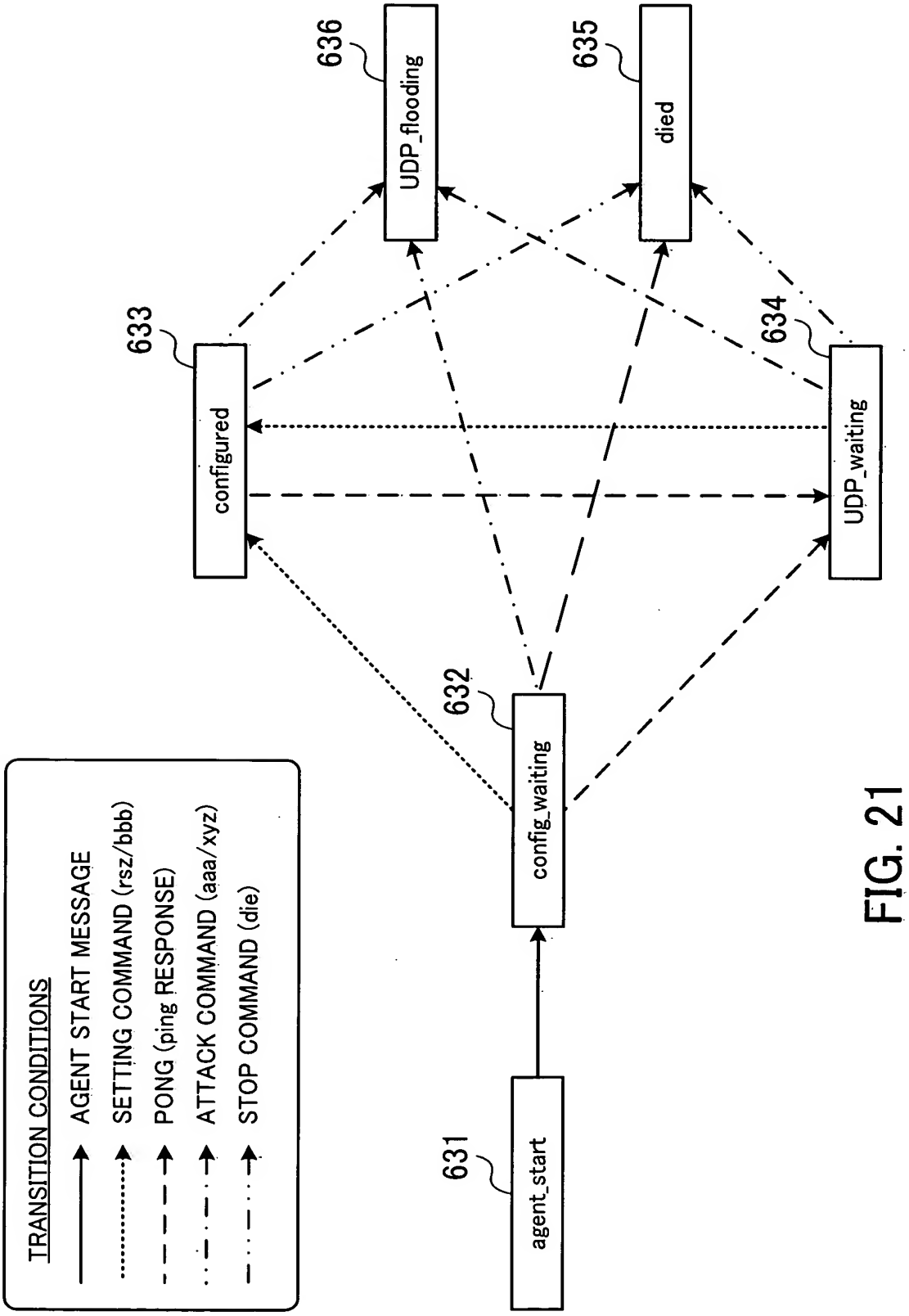

TRANSITION CONDITIONS
AGENT START MESSAGE
SETTING COMMAND (rsz/bbb)
PONG (ping RESPONSE)
ATTACK COMMAND (aaa/xyz)
STOP COMMAND (die)
631
agent_start
632
config_waiting
633
configured
634
UDP_waiting
635
died
636
UDP_flooding

FIG. 21

640 PREDICATED IMPACT/MEASURE DEFINITION TABLE

TIME TO IMPACT	POSSIBILITY OF IMPACT	SCALE OF IMPACT	PREVENTATIVE MEASURES
WITHIN 5 MINUTES	70%	LARGE	INTERRUPT COMMUNICATION FOR ONE HOUR (BECAUSE OF VERY URGENT AND LARGE IMPACT)
WITHIN 1 HOUR	10%	LARGE	
WITHIN ONE DAY	10%	MEDIUM	

FIG. 22

650 PREDICATED IMPACT /MEASURE DEFINITION TABLE

TIME TO IMPACT	POSSIBILITY OF IMPACT	SCALE OF IMPACT	PREVENTATIVE MEASURES
WITHIN 1 HOUR	10%	MEDIUM	NOTIFY THE ADMINISTRATOR OF A HOST (ADMINISTRATIOR HOST) THAT PROBABLY LAUNCHES AN ATTACK, MONITOR COMMUNICATION FOR NEXT 3 DAYS, AND INTERRUPT, IF NECESSARY, THE COMMUNICATION (BECAUSE IMPACT DOES NOT OCCUR SOON)
WITHIN 1 DAY	40%	LARGE	
WITHIN 3 DAYS	30%	LARGE	

FIG. 23